UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

UNITED STATES OF AMERICA,

v.

JONG SONG HWA (정성화),
RI KYONG SIK (리경식),
KIM RYU SONG (김류성),
RIM UN CHOL (림은철),
KIM MU RIM (김무림),
CHO CHUNG POM (조충범),
HYON CHOL SONG (현철성),
SON UN CHOL (손은철),
SOK KWANG HYOK (석광혁),
CHOE JONG YONG (최정용),
KO CHUNG SOK (고충석),
KIM YE WON (김예원),
JONG KYONG CHOL (정경철), and
JANG CHOL MYONG (장철명),

Defendants.

No: 4:24CR648 MTS/JSD

INDICTMENT

The Grand Jury charges that, at all times material to this Indictment:

GENERAL ALLEGATIONS

1. The United States maintains comprehensive trade and economic sanctions against the Government of the Democratic People's Republic of Korea (the "DPRK") due to the national security threats posed by the DPRK, including its nuclear weapons program. These sanctions have the effect of denying the DPRK access to the U.S. marketplace and financial system and restricting the ability of U.S. persons and companies to do business and otherwise transact with the DPRK.

As a result, the DPRK has carried out or sponsored various schemes to evade U.S. sanctions to generate funds.

2. According to a May 2022 advisory by the Department of State, the Department of the Treasury, and the Federal Bureau of Investigation, the DPRK has dispatched thousands of highly-skilled information technology ("IT") workers around the world, earning revenue that contributes to the DPRK's weapons programs, in violation of U.S. and UN sanctions. These workers: (i) misrepresent themselves as foreign (non-DPRK) or U.S.-based teleworkers, including by using virtual private networks ("VPNs"), virtual private servers ("VPSs"), third- country internet protocol ("IP") addresses, proxy accounts, and falsified or stolen identification documents; (ii) surreptitiously obtain IT development employment from companies spanning a range of sectors and industries around the world; (iii) develop applications and software for their employers; and (iv) in some instances, use privileged access gained through such employment for illicit purposes, including enabling malicious cyber intrusions by other DPRK actors into an employer's network.

3. According to the May 2022 advisory, all DPRK IT workers earn money to support their government. The vast majority of them are subordinate to and working on behalf of entities directly involved in the DPRK's UN-prohibited nuclear and ballistic missile programs, as well as its advanced conventional weapons development and trade sectors. DPRK entities dispatching IT workers include: (i) the Munitions Industry Department, which controls the DPRK's research and development and productions of weapons—to include nuclear weapons and ballistic missiles—and other military equipment; (ii) the Ministry of Atomic Energy Industry—a critical player in the DPRK's development of nuclear weapons and the day-to-day operations of the DPRK's nuclear weapons program; and (iii) military entities subordinate to the Ministry of Defense and Korea People's Army. These entities have been designated for sanctions by the United States.

4. From in or around April 2017 to in or around March 2023, the defendants, JONG SONG HWA (정성화), RI KYONG SIK (리경식), KIM RYU SONG (김류성), RIM UN CHOL (림은철), KIM MU RIM (김무림), CHO CHUNG POM (조충범), HYON CHOL SONG (현철성), SON UN CHOL (손은철), SOK KWANG HYOK (석광혁), CHOE JONG YONG (최정용), KO CHUNG SOK (고충석), KIM YE WON (김예원), JONG KYONG CHOL (정경철), and JANG CHOL MYONG (장철명), engaged in a conspiracy to violate and evade U.S. sanctions to raise revenue for the DPRK. The defendants, in various capacities, were associated with a sanctioned DPRK front company named Yanbian Silverstar Network Technology Co., Ltd. ("Yanbian Silverstar"), based in the People's Republic of China ("PRC"), and a sanctioned DPRK front company named Volasys Silverstar, based in the Russian Federation. In total, Yanbian Silverstar and Volasys Silverstar employed and retained at least 130 DPRK IT workers, known among the conspirators as "IT Warriors."

5. In furtherance of the conspiracy, the defendants used stolen, borrowed, and purchased identities of U.S. persons and foreign nationals to conceal their true identities as DPRK nationals and: (i) apply for and obtain remote employment as IT workers with U.S. businesses and organizations; (ii) register internet domain names used to host websites designed to trick U.S. employers into thinking IT worker applicants and employees were currently or previously employed by reputable U.S. businesses; and (iii) create money transfer service accounts to receive funds from their U.S. employers and remit those funds to PRC-based banks for eventual use by the DPRK.

6. The defendants also enlisted U.S. persons to purchase laptops or receive laptops from U.S. employers and install remote access programs on them. When the defendants remotely accessed such laptops, it would appear to the U.S. employers that the defendants were performing

assigned remote IT work from within the United States. When the defendants gained access to a U.S. employer's sensitive business information, the defendants in some instances extorted payments from the employer by threatening to release, and in some cases releasing, that sensitive information online.

7. Throughout the approximately six-year conspiracy, the defendants and their conspirators employed by Yanbian Silverstar and Volasys Silverstar fraudulently possessed and used the identities of hundreds of U.S. persons to generate at least $88 million in illicit revenue for the DPRK.

THE INTERNATIONAL EMERGENCY ECONOMIC POWERS ACT

8. The International Emergency Economic Powers Act ("IEEPA"), 50 U.S.C § 1701 *et seq.*, authorizes the President of the United States to impose trade and economic sanctions in response to an unusual and extraordinary threat to the national security, foreign policy, or economy of the United States. Pursuant to that authority, the President may declare a national emergency through Executive Orders that have the full force and effect of law. Under IEEPA, it is a crime to willfully violate, attempt to violate, conspire to violate, or cause a violation of any order, license, regulation, or prohibition issued pursuant to the statute. 50 U.S.C. § 1705.

9. Pursuant to IEEPA, the President and the Executive Branch have issued Executive Orders and regulations governing and prohibiting certain transactions involving the DPRK. Specifically, on June 26, 2008, the President issued Executive Order 13466, finding that that "the existence and risk of the proliferation of weapons-usable fissile material on the Korean Peninsula constituted an unusual and extraordinary threat to the national security and foreign policy of the United States" and declaring a "national emergency to deal with that threat." The President has imposed additional sanctions with respect to the DPRK. *See* Executive Orders 13551 (Aug. 30,

2010), 13570 (Apr. 18, 2011), 13722 (Mar. 15, 2016), and 13810 (Sept. 20, 2017). To implement these Executive Orders, the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") issued the North Korean Sanctions Regulations (the "NKSR"). 31 C.F.R. Part 510.

10. On March 15, 2016, the President, in order to take additional steps with respect to the national emergency described in Executive Order 13466, issued Executive Order 13722 to address the DPRK's continuing pursuit of its nuclear and missile programs. Among other things, Executive Order 13722 imposed a comprehensive blocking of the property and interests in property of the DPRK and the Workers' Party of Korea. As a result, U.S. persons, including U.S. financial institutions and companies, are generally prohibited from transacting with the DPRK.

11. On March 5, 2018, OFAC amended and reissued the NKSR in their entirety to implement Executive Order 13722, among others. 83 Fed. Reg. 9182 (Mar. 5, 2018). Absent permission from OFAC in the form of a license, the NKSR prohibits, among other things, the exportation or re-exportation, directly or indirectly, from the United States, or by a U.S. person, wherever located, of any goods, services, or technology to North Korea. 31 C.F.R. § 510.206(a); *see also* Executive Order 13722 § 3. This prohibition applies to services, including financial services, performed on behalf of a person in North Korea or the DPRK or where the benefit of such services is otherwise received in North Korea. 31 C.F.R. § 510.405. Additionally, the benefit of services performed anywhere in the world on behalf of the DPRK is presumed to be received in North Korea. *Id.* The NKSR also prohibits any transaction that evades or avoids, has the purpose of evading or avoiding, causes a violation of, or attempts to violate or any conspiracy formed to violate any of the prohibitions set forth in the NKSR. 31 C.F.R. § 510.212.

12. Further, Executive Orders 13722 and 13810 block all property and interests in property in the United States, or in the possession or control of any U.S. person, of persons

determined by the Secretary of the Treasury to meet specific enumerated criteria. The names of such persons are published in OFAC's Specially Designated Nationals and Blocked Persons ("SDN") List.

13. On September 13, 2018, pursuant to Executive Orders 13722 and 13810, OFAC designated Yanbian Silverstar and Volasys Silverstar and added them to the SDN List for having engaged in, facilitated, or been responsible for the exportation of workers from North Korea, including exportation to generate revenue for the DPRK or the Workers' Party of Korea, and for operating in the IT industry in North Korea. OFAC also designated a DPRK national, JONG SONG HWA, the leader of Yanbian Silverstar, and added him to the SDN List pursuant to Executive Order 13810 for having acted or purported to act for or on behalf of, directly or indirectly, Yanbian Silverstar.

THE CONSPIRATORS

14. JONG SONG HWA, a DPRK national, was the Mission Representative (or leader) of Yanbian Silverstar and Volasys Silverstar. As Mission Representative, JONG SONG HWA set the strategic goals of, and gave orders and direction to, managers and employees of Yanbian Silverstar and Volasys Silverstar. Among his orders and directions, JONG SONG HWA expected every IT worker at Yanbian Silverstar and Volasys Silverstar to generate at least $10,000 in revenue for the DPRK every month.

15. KIM RYU SONG, a DPRK national, was the "President" of Yanbian Silverstar.

16. RI KYONG SIK, a DPRK national, was the "President" of Volasys Silverstar.

17. KIM RYU SONG and RI KYONG SIK worked together to complete tasks assigned by JONG SONG HWA and to manage Yanbian Silverstar and Volasys Silverstar. JONG SONG HWA, KIM RYU SONG, and RI KYONG SIK made decisions together to motivate less

productive IT workers, reward top earning IT workers, promote IT workers to middle management, and transfer IT workers to and from North Korea. Among other things, JONG SONG HWA, KIM RYU SONG, and RI KYONG SIK organized periodic "socialism competitions," where Yanbian Silverstar and Volasys Silverstar IT workers would compete to generate money for the DPRK through IT work, and they awarded bonuses and other prizes to the top performers in the competition.

18. RIM UN CHOL, a DPRK national, was a "Delegation Leader" for Yanbian Silverstar. Delegation Leaders supervised Group Leaders and IT Workers to ensure they met the goals set by JONG SONG HWA, KIM RYU SONG, and RI KYONG SIK. Along with other Delegation Leaders, RIM UN CHOL managed the day-to-day operations of at least 50 DPRK IT workers in the PRC and reported to Yanbian Silverstar President KIM RYU SONG.

19. KIM MU RIM, a DPRK national, was a "Delegation Leader" for Yanbian Silverstar. Along with other Delegation Leaders, KIM MU RIM managed the day-to-day operations of at least 50 DPRK IT workers in the PRC and reported to Yanbian Silverstar President KIM RYU SONG.

20. CHO CHUNG POM, HYON CHOL SONG, SON UN CHOL, and SOK KWANG HYOK, all DPRK nationals, acted as middle management also known as "Group Leaders" for Yanbian Silverstar and reported to Delegation Leader RIM UN CHOL. The Group Leaders directly supervised IT workers and occasionally conducted IT work themselves.

21. CHOE JONG YONG, KO CHUNG SOK, KIM YE WON, JONG KYONG CHOL, and JANG CHOL MYONG (collectively referred to hereafter as the "Yanbian Employees"), all DPRK nationals, worked as IT workers for Yanbian Silverstar and reported to the Group Leaders.

THE CONSPIRACY

22. It was part of the conspiracy that the defendants and others known and unknown to the Grand Jury used the following manner and means, among others, to achieve the goals of the conspiracy.

Working for and Extorting U.S. Employers

23. The conspirators pretended to be U.S. persons seeking remote IT work by using stolen, borrowed, or purchased identities. In some instances, to better hide their identities and obtain employment, the conspirators paid U.S. persons and others to appear in their place at interviews and provided direction and guidance to the U.S. persons during the interviews. After being hired, the conspirators paid U.S. persons and others to receive and maintain laptops that were provided by U.S. businesses. By using U.S. persons to interview in their place and to host employer-provided laptops, the conspirators created the false appearance that employers had hired U.S. persons who were performing work from within the United States.

24. To further the deception and make their resumes appear more appealing, the conspirators claimed that they previously worked in similar roles for other U.S.-based companies. However, those companies were fake. To make the companies appear legitimate, the conspirators purchased and designed websites for them.

25. As part of their revenue-generation operations, in some instances, the conspirators extorted the U.S. businesses that hired them. They first gained access to sensitive or proprietary information and then threatened to publish, and in some cases did publish, that information if the businesses that hired them did not pay them a specified sum. At the direction of JONG SONG HWA, KIM RYU SONG, RI KYONG SIK, RIM UN CHOL, and KIM MU RIM, the Yanbian

Employees, Group Leaders, and other conspirators sent the salary or extortion payments they received to accounts controlled by the DPRK, including accounts at banks based in the PRC.

a. Yanbian Employees and Group Leaders Get Assigned and Use Stolen Identities

26. Between approximately February and March 2021, CHO CHUNG POM, CHOE JONG YONG, SON UN CHOL, KIM YE WON, and SOK KWANG HYOK were ordered to use Personally Identifiable Information ("PII") stolen from 188 U.S. persons. This information included names, dates of birth, social security numbers, and addresses and was held by CHOE JONG YONG (the "SSN LIST"). In several instances, CHO CHUNG POM, CHOE JONG YONG, SON UN CHOL, KIM YE WON, SOK KWANG HYOK, and conspirators known and unknown to the Grand Jury used the stolen PII in the SSN LIST in furtherance of their conspiracy.

27. Between approximately June 2017 and April 2022, KIM RYU SONG had multiple Chinese national identification cards, some of which were used by the conspirators to open or operate financial accounts at banks located in the PRC. The PRC-based banks received payments from U.S. money transfer service accounts owned and operated by the conspirators. The conspirators used U.S. identities to open and manage the U.S. money transfer service accounts. These U.S. money transfer service accounts received salary payments from the U.S. businesses and nonprofits that employed the conspirators as well as payments from U.S. businesses and nonprofits that the conspirators extorted.

b. U.S. Business #1

28. On or about September 19, 2019, to conceal their identities and appear to be U.S. persons, the conspirators paid A.P., a U.S. person, to appear at interviews with U.S. businesses using the name, date of birth, and social security number of M.A., a different U.S. person whose

identity was stolen. The conspirators initially agreed to pay A.P. at least $100 for each job interview and at least $20 an hour for other work.

29. On or about October 12, 2021, U.S. Business #1, a software development company located in Oregon, interviewed and hired an individual it believed to be M.A. to do contract IT work. M.A. was actually A.P. acting at the behest of KIM YE WON. To get the M.A. identity hired by U.S. Business #1, the conspirators used wire communications in interstate and foreign commerce. As part of its employment with U.S. Business #1, the M.A. identity, and through it the conspirators, was given access to proprietary information held by U.S. Business #1.

30. On or about October 16, 2021, KIM YE WON and SOK KWANG HYOK agreed to pay A.P. approximately $1,000 a week to impersonate M.A., thereby allowing KIM YE WON and SOK KWANG HYOK to regularly work for U.S. Business #1.

31. Between on or about September 19, 2019, and on or about April 24, 2023, A.P. received at least $69,900 from the conspirators. These funds were sent to A.P.'s account at a U.S. money transfer service ("U.S. MTS #1"), which A.P. created on or about September 19, 2021. KIM YE WON was responsible for most of A.P.'s payments, and KIM YE WON made these payments using an account at U.S. MTS #1, which was created with the name and identifying information of "J.C.," a U.S. person whose identity was borrowed.

32. On or about October 4, 2021, SOK KWANG HYOK used wire communications in interstate and foreign commerce to open an account at U.S. money transfer service #2 ("U.S. MTS #2") using the stolen name, date of birth, and social security number of M.A. As part of the account verification process, SOK KWANG HYOK provided U.S. MTS #2 with a fraudulent driver's license, which had M.A.'s personal information, but a picture of SOK KWANG HYOK.

33. Between approximately October 12, 2021, and February 18, 2022, U.S. Business #1 paid SOK KWANG HYOK, who worked with A.P. to pose as M.A., approximately $59,000. HYON CHOL SONG used wire communications in interstate and foreign commerce to open an account at U.S. MTS #2 using a Mexican identification document featuring the name M.L. The M.L. U.S. MTS #2 account received payments from U.S. Business #1 associated with the M.A. identity's employment.

34. Over four transactions between on or about November 26, 2021, and February 3, 2022, using the M.L. U.S. MTS #2 account, HYON CHOL SONG sent funds received from U.S. Business #1 to the U.S. MTS #2 account created in M.A.'s name but controlled by SOK KWANG HYOK.

35. On or about February 18, 2022, U.S. Business #1 terminated its relationship with the M.A. identity.

36. On or about March 7, 2022, SOK KWANG HYOK used wire communications in interstate and foreign commerce to pose as M.A. and demand that U.S. Business #1 send an additional $10,000 to the M.L. U.S. MTS #2 account. SOK KWANG HYOK stated that if the money was not paid, he would publicly post U.S. Business #1's proprietary business information. U.S. Business #1 refused to pay SOK KWANG HYOK.

37. On or about March 9, 2022, SOK KWANG HYOK used an account registered using the M.A. identity to post U.S. Business #1's proprietary information on a public website for software development, which caused hundreds of thousands of dollars in loss and damage to U.S. Business #1.

c. U.S. Business #2

38. In or around February 2022, HYON CHOL SONG used wire communications in interstate and foreign commerce to apply for a remote IT specialist position with U.S. Business #2, a talent hiring firm located in Texas. In his application, HYON CHOL SONG posed as M.H., a U.S. person, and used a falsified New York driver's license containing M.H.'s PII.

39. On or about March 21, 2022, U.S. Business #2 hired an individual it believed to be M.H to be a remote IT specialist. M.H. was actually HYON CHOL SONG. As part of its employment with U.S. Business #2, the M.H. identity, and through it HYON CHOL SONG, was given access to proprietary information held by U.S. Business #2.

40. Between in or around March 2022 and in or around February 2023, U.S. Business #2 paid HYON CHOL SONG, who posed as M.H., approximately $50,000. HYON CHOL SONG used wire communications in interstate and foreign commerce to open an account at U.S. MTS #2 using a Ukrainian identification document featuring the name O.C. The O.C. U.S. MTS #2 account received payments from U.S. Business #2 associated with the M.H. identity's employment.

41. HYON CHOL SONG used the O.C. U.S. MTS #2 account to send the salary that he received from U.S. Business #2 to two accounts at PRC Bank #1 (a bank based in the PRC).

42. On or about February 2023, U.S. Business #2 discovered that the M.H. identity controlled by HYON CHOL SONG was outsourcing his work to other individuals without its knowledge or permission. U.S. Business #2 terminated its relationship with the M.H. identity and demanded HYON CHOL SONG disclose the names of the individuals he was using to subcontract the work.

43. On or about March 2, 2023, and continuing until on or about March 17, 2023, HYON CHOL SONG used wire communications in interstate and foreign commerce to pose as M.H and demand that U.S. Business #2 send an additional approximately $2,200 to the O.C. U.S.

MTS #2 account. HYON CHOL SONG stated that if the money was not paid, he would publicly post U.S. Business #2's proprietary business information. U.S. Business #2 refused to pay HYON CHOL SONG.

44. On or about March 2, 2023, HYON CHOL SONG used an account registered using the M.H. identity to post U.S. Business #2's proprietary information on a public website for software development.

d. U.S. Business #3

45. On or about December 9, 2018, KO CHUNG SOK used wire communications in interstate and foreign commerce to apply for a position as a remote developer with U.S. Business #3, a company that owns and operates an application for identifying popular local businesses, located in North Carolina. In his application, KO CHUNG SOK posed as P.C., a U.S. person.

46. On or about December 10, 2018, U.S. Business #3 hired an individual it believed to be P.C. to be a remote developer. P.C. was actually KO CHUNG SOK.

47. Between in or around December 2018 and in or around July 2022, U.S. Business #3 paid KO CHUNG SOK, who posed as P.C., approximately $148,000. KO CHUNG SOK received these funds at a U.S. MTS #2 account that was created using a U.S.-based email service.

48. On or about July 4, 2022, U.S. Business #3 terminated its relationship with the P.C. identity due to poor work performance.

e. U.S. Business #4

49. In or around July 2021, CHOE JONG YONG created a resume in the name of R.W., a U.S. person whose PII was in the SSN LIST, to apply for jobs at various U.S. businesses using wire communications in interstate and foreign commerce.

50. In or around September 2021, CHOE JONG YONG used wire communications in interstate and foreign commerce to apply for an application developer position with U.S. Business #4, an internet streaming technology company located in Iowa. In his application, CHOE JONG YONG posed as R.W., a U.S. person.

51. On or about October 6, 2021, U.S. Business #4 interviewed an individual it believed to be R.W. for an application development role. R.W. was actually A.P. acting at the behest of CHOE JONG YONG. The same day, CHOE JONG YONG paid A.P. $100 for participating in the interview.

52. On or about October 18, 2021, U.S. Business #4 hired the individual it believed to be R.W.

53. Between on or about October 18, 2021, and on or about April 15, 2022, U.S. Business #4 paid CHOE JONG YONG, who posed as R.W., approximately $95,000. CHOE JONG YONG used wire communications in interstate and foreign commerce to open an account at U.S. MTS #2 using a U.S. identification document featuring the name J.H. J.H. is a U.S. person whose PII was in the SSN LIST. The J.H. U.S. MTS #2 account received payments from U.S. Business #4 associated with the R.W. identity's employment.

54. CHOE JONG YONG used the J.H. U.S. MTS #2 account to send approximately $20,000 of the salary the R.W. identity received from U.S. Business #4 to an account at PRC Bank #2 (a bank based in the PRC) and approximately $39,700 of the salary the R.W. identity received from U.S. Business #4 to an account at PRC Bank #1.

55. On or about April 15, 2022, U.S. Business #4 terminated its relationship with the R.W. identity.

f. U.S. Businesses #5 and #6

56. On or about May 25, 2021, JANG CHOL MYONG used wire communications in interstate and foreign commerce to open an account at U.S. MTS #2 using the name, date of birth, and social security number of J.S., a U.S. person. As part of the account verification process, JANG CHOL MYONG provided U.S. MTS #2 with a falsified driver's license containing J.S.'s name and PII.

57. On or about September 15, 2021, U.S. Business #5, a consulting and staffing company located in Washington, hired an individual it believed to be J.S. as a remote IT contractor. J.S. was actually JANG CHOL MYONG. To get the J.S. identity hired by U.S. Business #5, JANG CHOL MYONG used a falsified driver's license and other documents containing J.S.'s, name, date of birth, and social security number. As described generally in paragraph 23 above, to get hired by U.S. Business #5, JANG CHOL MYONG, who posed as J.S., claimed to have previously worked for BabyBox Tech, a fake company that claimed to be based in California. The fake company was associated with the website babyboxtech.com, and claimed to specialize in web design, graphic design, and branding.

58. On or about October 11, 2021, U.S. Business #5 assigned JANG CHOL MYONG, who posed as J.S., to a software development contract with U.S. Business #6, a technology company located in California.

59. On or about October 29, 2021, U.S. Business #6 terminated its relationship with the J.S. identity after learning that J.S.'s U.S. Business #6-provided laptop was accessed from the PRC on or about October 25, 2021.

60. JANG CHOL MYONG received a payment of approximately $2,000 from U.S. Business #6, which sent the funds through U.S. Business #5, prior to his termination. JANG

CHOL MYONG received this payment on or about October 29, 2021, at the J.S. U.S. MTS #2 account.

61. On or about October 29, 2021, JANG CHOL MYONG sent approximately $2,000 from the J.S. U.S. MTS #2 account to a different U.S. MTS #2 account in the name of W.D., an identity that purported to be a PRC national.

62. On or about November 1, 2021, the W.D. U.S. MTS #2 account sent the approximately $2,000 and other funds to an account at PRC Bank #3 (a bank based in the PRC).

g. U.S. Nonprofit Organization #1

63. In or around May 2021, CHO CHUNG POM used wire communications in interstate and foreign commerce to apply for a remote IT contractor position with U.S. Nonprofit Organization #1, a faith-based nonprofit organization located in Indiana. In his application, CHO CHUNG POM posed as E.H., a U.S. person whose PII was in the SSN LIST.

64. On or about June 7, 2021, U.S. Nonprofit Organization #1 hired an individual it believed to be E.H. for the position. E.H. was actually CHO CHUNG POM. As part of its employment with U.S. Nonprofit Organization #1, the E.H. identity, and through it CHO CHUNG POM, was given access to proprietary information held by U.S. Nonprofit Organization #1.

65. On or about June 22, 2021, U.S. Nonprofit Organization #1 terminated its relationship with the E.H. identity.

66. On or about June 22, 2021, CHO CHUNG POM used wire communications in interstate and foreign commerce to pose as E.H. and demand that U.S. Nonprofit Organization #1 pay his salary for work that he claimed to have performed during the prior pay period. CHO CHUNG POM stated that if the money was not paid, he would post U.S. Nonprofit Organization #1's proprietary information. CHO CHUNG POM used an account registered using the E.H.

identity to post U.S. Nonprofit Organization #1's proprietary information on a public website for software development.

67. On or about June 22, 2021, U.S. Nonprofit Organization #1 paid CHO CHUNG POM $2,730 by sending funds to a U.S. MTS #1 account created using the stolen PII of E.E., a U.S. person. CHO CHUNG POM then removed the source code from the software development website.

68. To hide his true location while seeking and maintaining employment with U.S. businesses and nonprofit organizations, CHO CHUNG POM remotely accessed a laptop owned and operated by E.J. That laptop was located in St. Louis, Missouri. CHO CHUNG POM had previously recruited E.J. and instructed E.J. to acquire a laptop and install a remote access program.

69. On or about June 25, 2021, CHO CHUNG POM, using E.J.'s laptop located in the Eastern District of Missouri, transferred funds from an U.S. MTS #1 account held in E.E.'s name to a U.S. MTS #1 account held in the name R.T., an identity affiliated with a U.S. person, that was controlled by KIM YE WON.

h. U.S. Nonprofit Organization #2

70. On or about December 3, 2019, to conceal their identities and appear to be non-DPRK citizens, CHOE JONG YONG and SON UN CHOL paid B.T., a Belgian person, approximately $130 in order to use B.T.'s identity to obtain freelance IT work in the United States.

71. On or about January 22, 2020, U.S. Nonprofit Organization #2, an organization focused on child mental health and learning disorders located in New York, hired an individual it believed to be B.T. B.T. was actually CHOE JONG YONG.

72. As described generally in paragraph 23 above, to get hired by U.S. Nonprofit #2, CHOE JONG YONG, who posed as B.T., claimed to have previously worked for LJD Tech, a fake

company that claimed to be based in the United States, but had no website or state corporate registration.

73. Between on or about January 22, 2020, and on or about July 15, 2022, U.S. Nonprofit Organization #2 paid CHOE JONG YONG, who posed as B.T., at least $158,000. CHOE JONG YONG used wire communications in interstate and foreign commerce to open an account at U.S. MTS #2 using the B.T. identity. The B.T. U.S. MTS #2 account received payments from U.S. Nonprofit Organization #2 associated with the B.T. identity's employment.

74. On or about July 15, 2022, U.S. Nonprofit Organization #2 terminated its relationship with the B.T. identity after learning from the FBI that the B.T. identity was being controlled by a DPRK IT worker.

Use of Front Companies and Domains

75. The conspirators used multiple methods to increase their appeal to and *bona fides* with prospective U.S.-based employers. One such method was to register domain names and create associated websites that appeared to belong to legitimate U.S.-based businesses that hired out or otherwise supplied contractor freelance IT workers. These businesses did not actually exist. The conspirators would claim in their resumes, applications, or interviews that they had previously worked for these fake businesses.

76. The names of some of these fake businesses included Eden Programming Solutions, Purpleish Tech, Culture Box, Next Nets, Illusion Software, BabyBox Tech, Cubix Tech, and Helix. The domains hosting websites for these fake companies were, respectively, edenprogram.com, purpleishtech.com, culturebx.com, nextnets.com, illusionsoft.net, babyboxinfo.com, babyboxtech.com, cubixtechus.com, and helix-us.com.

77. On or about June 26, 2020, HYON CHOL SONG, using the identity of M.K., a U.S. person, registered the domain edenprogram.com from U.S. Domain Registrar #1. The website at that domain falsely claimed that Eden Programming Solutions provided clients with web development expertise and was based in the United States.

78. On or about January 25, 2021, JANG CHOL MYONG, using the identity H.E., registered the domain babyboxtech.com from U.S. Domain Registrar #2. The website claimed the company BabyBox Tech was a certified software development studio and was based in California.

79. On or about May 13, 2022, JONG KYONG CHOL, using the S.G. identity, registered the domain culturebx.com from U.S. Domain Registrar #1. The website at that domain falsely claimed that Culture Box specialized in business analytics and was based in Oklahoma. An entity with the same name that claimed to be linked to the same website also was registered with the Secretary of State of Wyoming (a registration that was later terminated by the State of Wyoming following a FBI notification).

80. On or about March 7, 2023, JONG KYONG CHOL, using the identity of S.G., a U.S. person, registered the domain nextnets.com from U.S. Domain Registrar #1. The website at that domain falsely claimed that Next Nets specialized in cloud computing and artificial intelligence and was based in Richmond, Virginia.

81. On or about August 2, 2023, JONG KYONG CHOL, using the S.G. identity, registered the domain purpleishtech.com from U.S. Domain Registrar #1. The website at that domain falsely claimed that Purpleish Tech had expertise in cloud solutions and mobile app development and was based in Texas.

82. On or about October 17, 2023, HYON CHOL SONG, using the identity M.K., registered the domain illusionsoft.net from U.S. Domain Registrar #1. The website at that domain

falsely claimed that Illusion Software specialized in web development and IT management and had been in operation since 2015.

83. On or about February 3, 2022, January 22, 2022, and January 27, 2022, JONG KYONG CHOL, using the identity J.S., registered the domains babyboxinfo.com, cubixtechus.com, and helix-us.com, respectively, from U.S. Domain Registrar #2. The website babyboxinfo.com falsely claimed that BabyBox Tech specialized in web design, graphic design, and branding and was based in New York. The website cubixtechus.com falsely claimed that Cubix Tech specialized in mobile web development and was based in Indiana. The website helix-us.com falsely claimed that Helix specialized in software implementation and was based in Michigan.

COUNT 1

(Conspiracy to Violate the International Emergency Economic Powers Act)

84. The allegations contained in paragraphs 1 through 83 above are re-alleged and incorporated here as if fully set forth herein.

85. From in or around April 2017 to in or around March 2023, in the Eastern District of Missouri and elsewhere,

JONG SONG HWA (정성화),

RI KYONG SIK (리경식),

KIM RYU SONG (김류성),

RIM UN CHOL (림은철),

KIM MU RIM (김무림),

CHO CHUNG POM (조충범),

HYON CHOL SONG (현철성),

SON UN CHOL (손은철),

SOK KWANG HYOK (석광혁),

CHOE JONG YONG (최정용),

KO CHUNG SOK (고충석),

KIM YE WON (김예원),

JONG KYONG CHOL (정경철), and

JANG CHOL MYONG (장철명),

defendants, and others known and unknown to the Grand Jury, did knowingly and willfully combine, conspire, confederate, and agree to export, and cause U.S. persons and entities to export and reexport, goods and services to North Korea, without prior authorization or license from the U.S. Department of the Treasury.

86. The objects of the conspiracy were, among others, to evade U.S. sanctions and generate revenue for the DPRK by obtaining U.S. employment for DPRK IT workers through the use of false identities. In furtherance of these objects, the managers of Yanbian Silverstar and Volasys Silverstar monitored the performance of the IT workers across several categories; in particular, the number of job interviews, jobs obtained, revenue generated, accounts created at money transfer service and freelance work platforms, and U.S. persons recruited to sell their identities or provide other services to the IT workers.

87. In the course of Count 1, HYON CHOL SONG, JONG KYONG CHOL, JANG CHOL MYONG, and other conspirators known and unknown to the Grand Jury, did knowingly, and in furtherance of the goals of the conspiracy, use fictitious and fraudulent aliases to falsely register domains, and did knowingly used those domains to create websites designed to support the false information that the conspirators provided to U.S. businesses and not-for-profits in order to be hired and paid, thereby causing those U.S. entities to violate U.S. sanction laws.

(All in violation of 50 U.S.C. § 1705, Executive Order 13722, and 31 C.F.R. §§ 510.206 and 510.212 and 18 U.S.C. § 3559(g)(1).)

COUNT 2
(Conspiracy to Commit Wire Fraud)

88. The allegations contained in paragraphs 1 through 87 above are re-alleged and incorporated here as if fully set forth herein.

89. From in or around April 2017 to in or around March 2023, in the Eastern District of Missouri and elsewhere,

JONG SONG HWA (정성화),

RI KYONG SIK (리경식),

KIM RYU SONG (김류성),

RIM UN CHOL (림은철),

KIM MU RIM (김무림),

CHO CHUNG POM (조충범),

HYON CHOL SONG (현철성),

SON UN CHOL (손은철),

SOK KWANG HYOK (석광혁),

CHOE JONG YONG (최정용),

KO CHUNG SOK (고충석),

KIM YE WON (김예원),

JONG KYONG CHOL (정경철), and

JANG CHOL MYONG (장철명),

defendants, and other conspirators known and unknown to the Grand Jury, did knowingly and willfully combine, conspire, confederate and agree together and with each other to commit wire fraud, that is having devised and intending to devise any scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, transmits and caused to be transmitted by means of wire, communication in interstate and foreign commerce, any writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice and in violation of 18 U.S.C. § 1343.

(All in violation of 18 U.S.C. § 1349.)

COUNT 3
(Money Laundering Conspiracy)

90. The allegations contained in paragraphs 1 through 89 above are re-alleged and incorporated here as if fully set forth herein.

91. As described above, members of the conspiracy obtained payments from businesses in exchange for IT work or after threatening to release sensitive information held by those businesses. Such payments were frequently made by Automated Clearing House ("ACH") transfers between financial services companies. Once money was received from those companies, money was often wired or transferred to banks in the PRC.

92. From in or around April 2017 to in or around March 2023, in the Eastern District of Missouri and elsewhere,

JONG SONG HWA (정성화),

RI KYONG SIK (리경식),

KIM RYU SONG (김류성),

RIM UN CHOL (림은철),

KIM MU RIM (김무림),

CHO CHUNG POM (조충범),

HYON CHOL SONG (현철성),

SON UN CHOL (손은철),

SOK KWANG HYOK (석광혁),

CHOE JONG YONG (최정용),

KO CHUNG SOK (고충석),

KIM YE WON (김예원),

JONG KYONG CHOL (정경철), and

JANG CHOL MYONG (장철명),

defendants, did knowingly combine, conspire, and agree with each other and other persons, known and unknown to the Grand Jury, to knowingly conduct and attempt to conduct financial transactions affecting interstate and foreign commerce, which involved the proceeds of specified unlawful activity, that is, conspiracy to commit wire fraud, in violation of 18 U.S.C. § 1349, and conspiracy to violate IEEPA, in violation of 50 U.S.C. § 1705. The defendants did this knowing that the transactions were designed in whole and in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of such specified unlawful activity, and that, while conducting the financial transactions, the defendants knew that the property involved in the financial transactions represented the proceeds of some form of unlawful activity, in violation of 18 U.S.C. § 1956(a)(1)(B)(i).

(All in violation of 18 U.S.C. § 1956(h).)

COUNT 4
(Conspiracy to Commit Identity Theft)

93. The allegations contained in paragraphs 1 through 92 above are re-alleged and incorporated here as if fully set forth herein.

94. From in or around April 2017 to in or around March 2023, in the Eastern District of Missouri and elsewhere,

JONG SONG HWA (정성화),

RI KYONG SIK (리경식),

KIM RYU SONG (김류성),

RIM UN CHOL (림은철),

KIM MU RIM (김무림),

CHO CHUNG POM (조충범),

HYON CHOL SONG (현철성),

SON UN CHOL (손은철),

SOK KWANG HYOK (석광혁),

CHOE JONG YONG (최정용),

KO CHUNG SOK (고충석),

KIM YE WON (김예원),

JONG KYONG CHOL (정경철), and

JANG CHOL MYONG (장철명),

defendants, did knowingly combine, conspire, and agree with each other and other persons, known and unknown to the Grand Jury, to transfer, possess and use, without lawful authority, in and affecting interstate and foreign commerce, the means of identification of another person, with the

intent to commit, and to aid and abet, and in connection with, any unlawful activity that constitutes a violation of Federal Law, to wit, the felony offenses of conspiracy to commit wire fraud in violation of 18 U.S.C. § 1349, conspiracy to conduct concealment money laundering in violation of 18 U.S.C. § 1956(h), and conspiracy to violate IEEPA, in violation of 50 U.S.C. § 1705, in violation of 18 U.S.C. § 1028(a)(7).

Overt Acts

95. In furtherance of the conspiracy, and to accomplish the objects thereof, defendants committed the following overt acts, among others, within the Eastern District of Missouri and elsewhere:

a. On or about December 9, 2018, KO CHUNG SOK applied for a position as a remote developer with U.S. Business #3 using PII associated with P.C.

b. On or about June 26, 2020, HYON CHOL SONG registered the domain edenprogram.com from U.S. Domain Registrar #1, using the M.K. identity.

c. On or about January 25, 2021, JANG CHOL MYONG registered the domain babyboxtech.com from U.S. Domain Registrar #2 using the H.E. identity.

d. On or about May 25, 2021, JANG CHOL MYONG created an account at U.S. MTS #2 using the driver's license, date of birth, and social security number of J.S.

e. In or around May 2021, CHO CHUNG POM applied for a remote IT contractor position with U.S. Nonprofit Organization #1, a faith-based nonprofit organization located in Indiana, using PII associated with E.H.

f. In or around September 2021, CHOE JONG YONG applied for an application developer position with U.S. Business #4, an internet streaming technology company located in Iowa, using PII associated with R.W.

g. On or about October 4, 2021, SOK KWANG HYOK opened an account at U.S. MTS #2 using the stolen name, date of birth, and social security number of M.A. As part of the account verification process, SOK KWANG HYOK provided U.S. MTS #2 with a fraudulent driver's license, which had M.A.'s personal information, but a picture of SOK KWANG HYOK.

h. On or about February 3, 2022, January 22, 2022, and January 27, 2022, JONG KYONG CHOL registered the domains babyboxinfo.com, cubixtechus.com, and helix-us.com, respectively, from U.S. Domain Registrar #2 using the J.S. identity.

i. In or around February 2022, HYON CHOL SONG applied for a remote IT specialist position with U.S. Business #2 using PII associated with M.H.

j. On or about May 13, 2022, JONG KYONG CHOL registered the domain culturebx.com from U.S. Domain Registrar #1 using the S.G. identity.

k. On or about March 7, 2023, JONG KYONG CHOL registered the domain nextnets.com from U.S. Domain Registrar #1 using the S.G identity.

l. On or about August 2, 2023, JONG KYONG CHOL registered the domain purpleishtech.com from U.S. Domain Registrar #1 using the S.G. identity.

m. On or about October 17, 2023, HYON CHOL SONG registered the domain illusionsoft.net from U.S. Domain Registrar #1 using the M.K. identity.

(All in violation of 18 U.S.C. § 371.)

COUNT 5
(Aggravated Identity Theft)

96. The allegations contained in paragraphs 1 through 95 above are re-alleged and incorporated here as if fully set forth herein.

97. From in or around April 2017 to in or around March 2023, in the Eastern District of Missouri and elsewhere,

CHO CHUNG POM (조충범),

HYON CHOL SONG (현철성),

SOK KWANG HYOK (석광혁),

CHOE JONG YONG (최정용),

KO CHUNG SOK (고충석),

KIM YE WON (김예원),

JONG KYONG CHOL (정경철), and

JANG CHOL MYONG (장철명),

defendants, did knowingly transfer, possess and use, without lawful authority, the means of identification of another person, during and in relation to the commission of the felony offense of conspiracy to commit wire fraud in violation of 18 U.S.C. § 1349, knowing that the means of identification belonged to an actual person.

(All in violation of 18 U.S.C. § 1028A(a).)

FORFEITURE ALLEGATIONS

The Grand Jury further finds by probable cause that:

98. Pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461, upon conviction of an offense in violation of Title 50, United States Code, Section 1705, as set forth in Count 1, or Title 18, United States Code, Section 1349, as set

forth in Count 2, or Title 18, United States Code, Section 371, as set forth in Count 4, the defendant(s) shall forfeit to the United States of America any property, real or personal, constituting or derived from proceeds traceable to said violation. Subject to forfeiture is a sum of money equal to the total value of any property, real or personal, constituting or derived from any proceeds traceable to said violations charged in Counts 1, 2 and 4.

99. Pursuant to Title 18, United States Code, Sections 982(a), upon conviction of an offense in violation of Title 18, United States Code, Section 1956, as set forth in Count 3, the defendant(s) shall forfeit to the United States of America any property, real or personal, involved in such offense, or any property traceable to such property. Subject to forfeiture is a sum of money equal to the total value of any property, real or personal, involved in such offense, or any property traceable to such property, for the violation charged in Count 3.

100. Specific property subject to forfeiture includes, but is not limited to, the following:

a. $230,451.28 in U.S. dollars seized from U.S. MTS #2 account ending in #7138;
b. $79,400.84 in U.S. dollars seized from U.S. MTS #2 account ending in #3195;
c. $75,054.35 in U.S. dollars seized from U.S. MTS #2 account ending in #4278;
d. $73,258.78 in U.S. dollars seized from U.S. MTS #2 account ending in #1057;
e. $45,934.74 in U.S. dollars seized from U.S. MTS #2 account ending in #8625;
f. $36,413.40 in U.S. dollars seized from U.S. MTS #2 account ending in #2927;
g. $33,190.57 in U.S. dollars seized from U.S. MTS #2 account ending in #2116;
h. $27,810.94 in U.S. dollars seized from U.S. MTS #2 account ending in #1354;
i. $25,134.92 in U.S. dollars seized from U.S. MTS #2 account ending in #2963;
j. $24,976.32 in U.S. dollars seized from U.S. MTS #2 account ending in #9922;
k. $22,972.28 in U.S. dollars seized from U.S. MTS #2 account ending in #6624;

l. $19,128.39 in U.S. dollars seized from U.S. MTS #2 account ending in #2110;

m. $18,776.61 in U.S. dollars seized from U.S. MTS #2 account ending in #0879;

n. $14,111.60 in U.S. dollars seized from U.S. MTS #2 account ending in #1935;

o. $9,361.25 in U.S. dollars seized from U.S. MTS #2 account ending in #5158;

p. $7,245.00 in U.S. dollars seized from U.S. MTS #2 account ending in #6723;

q. $6,115.55 in U.S. dollars seized from U.S. MTS #2 account ending in #3961;

r. $6,071.58 in U.S. dollars seized from U.S. MTS #2 account ending in #6635;

s. $3,743.36 in U.S. dollars seized from U.S. MTS #2 account ending in #6016;

t. $3,368.60 in U.S. dollars seized from U.S. MTS #2 account ending in #5450;

u. $2,711.49 in U.S. dollars seized from U.S. MTS #2 account ending in #2633;

v. $1,739.80 in U.S. dollars seized from U.S. MTS #2 account ending in #7501;

w. $1,447.26 in U.S. dollars seized from U.S. MTS #2 account ending in #9311;

x. $1,292.79 in U.S. dollars seized from U.S. MTS #2 account ending in #9276;

y. $1,120.65 in U.S. dollars seized from U.S. MTS #2 account ending in #1223;

z. $1,227.53 in U.S. dollars seized from U.S. MTS #2 account ending in #5264;

aa. $64,732.55 in U.S. dollars seized from U.S. MTS #2 account ending in #4410;

bb. $14,222.00 in U.S. dollars seized from U.S. MTS #2 account ending in #4950;

cc. $12,492.28 in U.S. dollars seized from U.S. MTS #2 account ending in #5342;

dd. $21,537.22 in U.S. dollars seized from U.S. MTS #2 account ending in #6965;

ee. $20,001.90 in U.S. dollars seized from U.S. MTS #2 account ending in #9874;

ff. $5,212.33 in U.S. dollars seized from U.S. MTS #2 account ending in #4884;

gg. $27,962.19 in U.S. dollars seized from U.S. MTS #2 account ending in #2701;

hh. $18,514.78 in U.S. dollars seized from U.S. MTS #2 account ending in #7047;

ii. $11,383.57 in U.S. dollars seized from U.S. MTS #2 account ending in #1277;

jj. $45,533.12 in U.S. dollars seized from U.S. MTS #2 account ending in #0481;

kk. $1,000.00 in U.S. dollars seized from U.S. MTS #2 account ending in #9452;

ll. $13,067.59 in U.S. dollars seized from U.S. MTS #2 account ending in #8330;

mm. $216.83 in U.S. dollars seized from U.S. MTS #2 account ending in #5387;

nn. $7,038.10 in U.S. dollars seized from U.S. MTS #2 account ending in #2708;

oo. $16,946.33 in U.S. dollars seized from U.S. MTS #2 account ending in #7034;

pp. $11,774.00 in U.S. dollars seized from U.S. MTS #2 account ending in #9187;

qq. $32,971.26 in U.S. dollars seized from U.S. MTS #2 account ending in #1426;

rr. $60,000.00 in U.S. dollars seized from U.S. MTS #2 account ending in #1348;

ss. $50,867.63 in U.S. dollars seized from U.S. MTS #2 account ending in #9184;

tt. $182.00 in U.S. dollars seized from U.S. MTS #2 account ending in #8285;

uu. $37,368.93 in U.S. dollars seized from U.S. MTS #2 account ending in #5868;

vv. $33,024.13 in U.S. dollars seized from U.S. MTS #2 account ending in #0229;

ww. $23,920.60 in U.S. dollars seized from U.S. MTS #2 account ending in #8706;

xx. $19,018.68 in U.S. dollars seized from U.S. MTS #2 account ending in #3213;

yy. $18,075.00 in U.S. dollars seized from U.S. MTS #2 account ending in #2641;

zz. $17,431.24 in U.S. dollars seized from U.S. MTS #2 account ending in #9486;

aaa. $14,031.76 in U.S. dollars seized from U.S. MTS #2 account ending in #8284;

bbb. $11,221.10 in U.S. dollars seized from U.S. MTS #2 account ending in #2914;

ccc. $10,000.00 in U.S. dollars seized from U.S. MTS #2 account ending in #1814;

ddd. $9,130.00 in U.S. dollars seized from U.S. MTS #2 account ending in #5130;

eee. $2,259.62 in U.S. dollars seized from U.S. MTS #2 account ending in #4106;

fff. $7,232.86 in U.S. dollars seized from U.S. MTS #2 account ending in #8551;

ggg. $9,740.52 in U.S. dollars seized from U.S. MTS #2 account ending in #4076;

hhh. $14,881.76 in U.S. dollars seized from U.S. MTS #2 account ending in #1566;

iii. $6,444.32 in U.S. dollars seized from U.S. MTS #2 account ending in #1644;

jjj. $6,398.23 in U.S. dollars seized from U.S. MTS #2 account ending in #2803;

kkk. $328.65 in U.S. dollars seized from U.S. MTS #2 account ending in #0755;

lll. $17,280.27 in U.S. dollars seized from U.S. MTS #2 account ending in #4382;

mmm. $4,343.62 in U.S. dollars seized from U.S. MTS #2 account ending in #0506;

nnn. $3,967.00 in U.S. dollars seized from U.S. MTS #2 account ending in #1742;

ooo. $452.63 in U.S. dollars seized from U.S. MTS #2 account ending in #6482;

ppp. $3,500.00 in U.S. dollars seized from U.S. MTS #2 account ending in #0570;

qqq. $2,631.20 in U.S. dollars seized from U.S. MTS #2 account ending in #9824;

rrr. $2,789.14 in U.S. dollars seized from U.S. MTS #2 account ending in #7596;

sss. $1,726.96 in U.S. dollars seized from U.S. MTS #2 account ending in #6453;

ttt. $2,140.00 in U.S. dollars seized from U.S. MTS #2 account ending in #1940;

uuu. $473.13 in U.S. dollars seized from U.S. MTS #2 account ending in #2372;

vvv. $3,189.85 in U.S. dollars seized from U.S. MTS #2 account ending in #1038;

www. $1,529.52 in U.S. dollars seized from U.S. MTS #2 account ending in #0482;

xxx. $154.99 in U.S. dollars seized from U.S. MTS #2 account ending in #1507;

yyy. $1,176.40 in U.S. dollars seized from U.S. MTS #2 account ending in #1486;

zzz. $753.58 in U.S. dollars seized from U.S. MTS #2 account ending in #4210;

aaaa. $286,808.48 in U.S. dollars seized from U.S. MTS #2 account ending in #6178;

bbbb. $25,834.07 in U.S. dollars seized from U.S. MTS #2 account ending in #6333;

cccc. $10,358.52 in Canadian dollars seized from U.S. MTS #2 account ending in #3548;

dddd. $239,862.37 in U.S. dollars and $65.31 in Euros seized from U.S. MTS #2 account ending in #6449;

eeee. $135,680.05 in U.S. dollars and $909.09 in Canadian dollars seized from U.S. MTS #2 account ending in #9820;

ffff. $16,537.21 in U.S. dollars seized from U.S. MTS #2 account ending in #2706;

gggg. $14,999.24 in U.S. dollars seized from U.S. MTS #2 account ending in #6036;

hhhh. $9,509.43 in U.S. dollars seized from U.S. MTS #2 account ending in #2749;

iiii. $8,690.83 in U.S. dollars seized from U.S. MTS #2 account ending in #8982;

jjjj. $6,734.61 in U.S. dollars and $0.91 in Euros seized from U.S. MTS #2 account ending in #8468;

kkkk. $6,142.31 in U.S. dollars seized from U.S. MTS #2 account ending in #0248;

llll. $5,681.00 in U.S. dollars seized from U.S. MTS #2 account ending in #7094; and

mmmm. The following domain names:

i. silverstarchina.com
ii. edenprogram.com
iii. xinlusoft.com
iv. foxysun.com
v. foxysunstudio.com
vi. foxysunstudios.com
vii. cloudbluefox.com
viii. cloudfoxhub.com
ix. mycloudfox.com
x. thefoxcloud.com
xi. thefoxesgroup.com
xii. babyboxtech.com
xiii. cloudfox.cloud
xiv. danielliu.info
xv. jinyang.asia
xvi. jinyang.services
xvii. ktsolution.tech
xviii. babyboxinfo.com
xix. blackishtech.com
xx. bynolt.com
xxi. cubixtechus.com
xxii. culturebx.com
xxiii. helix-us.com
xxiv. illusionsoft.net
xxv. logictech-us.com

xxvi. nextnets.com
xxvii. purpleishtech.com
xxviii. omegasoftware.us
xxix. thefox.cloud

101. If any of the property described above, as a result of any act or omission of the defendant(s):

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty,

the United States of America will be entitled to the forfeiture of substitute property pursuant to Title 21, United States Code, Section 853(p).

Dated: _____

A TRUE BILL.

_____
FOREPERSON

SAYLER A. FLEMING
United States Attorney

MATTHEW G. OLSEN
Assistant Attorney General for National Security

_____
Matthew T. Drake, #46499MO
Assistant United States Attorney

_____
Jacques Singer-Emery
Trial Attorney
Alexandra Cooper-Ponte
Trial Attorney